SCORE
FOR THE LIFE OF YOUR BUSINESS
Prairie and Lakes

Cyber Security for NonProfits

What We Will Cover Today:

- Understanding the Threat Environment & Why it Matters
- Where to Start
- *Resources Available to You*

Who Am I

Successfully Managing Our Clients Business Technology Systems since 1995

Rick Johnston

Retired President / Founder

At Information Management Systems, we Transform Business Technology into *Systems That Just Work ~ and Work Securely ~*

NASH

THE WHITE HOUSE
WASHINGTON

February 14, 1990

Dear Richard:

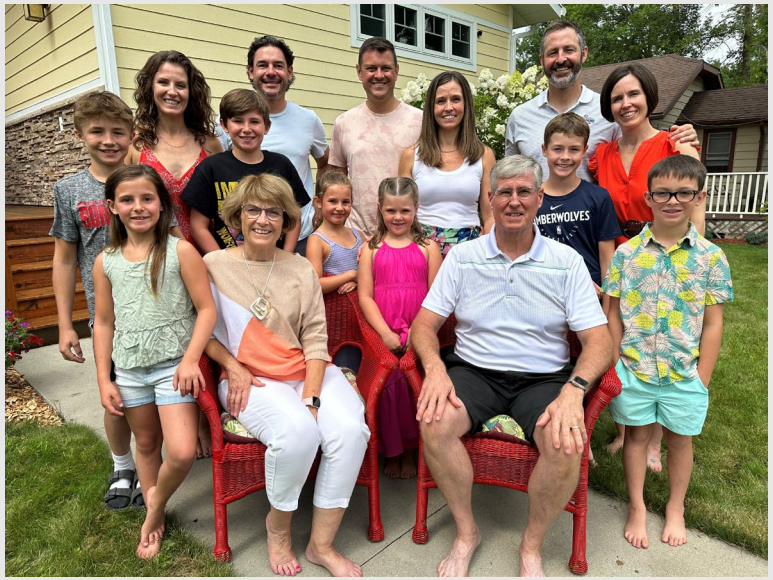
Congratulations on being selected as one of the nation's Outstanding Young Farmers for 1989 by the United States Jaycees.

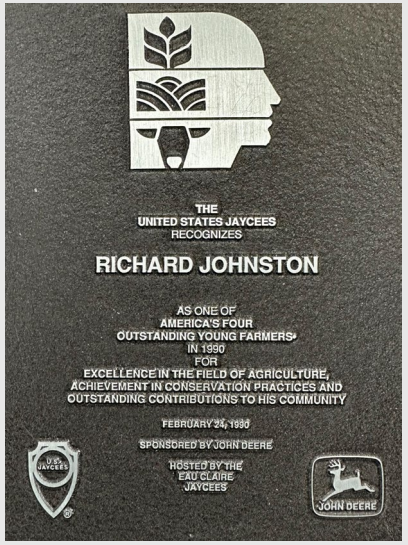
You can take great pride in this cherished tribute; it says a great deal about your vision, your enterprise, and your leadership. Your dedication to conserving this nation's fertile soil and your innovative ideas in agriculture, together with your volunteer spirit of service, clearly demonstrate your many talents and your love of community and country. You have made me and many Americans proud.

Again, congratulations and best wishes for the years to come. God bless you and your family.

Sincerely,

Mr. Richard Johnston
Route 2, Box 65
Grafton, North Dakota 58237





Information Management Systems
Computers & Networking

It could happen to anyone…don't let your business be next

Is This YOU?

Does your Nonprofit:

1. Conduct e-commerce on its website, such as processing donations or event registrations?

2. Store and transfer (such as by sending to the cloud) “personally identifiable information”, about anyone, including donors?

3. Collect information on preferences and habits of donors, patrons, newsletter subscribers, etc.?

Alarming statistics –

***Source:* *The State of Ransomware 2023* –**

Sophos, Jan - May 2023

Findings from an independent, vendor-agnostic survey of 3000 leaders responsible for IT/cybersecurity across 14 countries

- *66% -* hit by ransomware in the last year while *the average ransom payment almost DOUBLED from $812,360 to $1.54M*
- *76% -* attacks resulted in data encryption (up from 65%)
- 30% - ransomware attacks where data was encrypted reported that data was also stolen
- *97% -* got some encrypted data back
- *70% -* used data backups to restore data
- *46% -* paid the ransom and got data back
- *1% -* that paid the ransom got NO data back
- *84% -* ransomware attack impacted their ability to operate
- *61% - paid the ransom report it took ONE Month or LONGER – to recover data from an attack (55% for those who used backups)*

Small & Medium Businesses Experience Incidents and Breaches *MORE FREQUENTLY* Than Enterprise Businesses

Every layered security strategy must include something to protect personnel from their own mistakes.

Small organizations are especially at risk, with **inadequate** resources devoted to cybersecurity.

Security Incident

Incident is a security event that has been determined to have an impact on the organization prompting the need for response and recovery. It involves the compromise of the **CIA Triad (Confidentiality, Integrity, and Availability)**

Confidentiality

Incidents involving unauthorized access to systems or data, including privileged account compromise.

Integrity

Incidents involving data compromises, including leveraging a privileged account to corrupt or modify data.

Availability

Incidents that impact the availability of data or proper functioning of services, such as lost laptop containing data , Distributed Denial of Service (DDoS) or ransomware, including use of privileged account to make unauthorized changes.

When Privileged Accounts are involved the level of risk increases exponentially.

Security Breach

Breach is a type of security incident that involves the **release** of personally identifiable, protected and/or confidential data, such as:

- Medical information
- Drivers' licenses
- Addresses
- Social security numbers
- Email addresses
- Phone numbers
- Personal tastes/habits

According to the **2023 Cost of a Data Breach Report** by IBM and the Ponemon Institute, the global average cost of a data breach in 2023 was **$4.45 million** [123]. This is a **15% increase** over the past three years [1].

The report also highlights that the average cost per lost or stolen record containing sensitive and confidential information is **$165** [4].

Phishing Email Example #1

Re;:Approved ACH Payment No.02958117 Tuesday-September-2023 14:34 PM

PD

Payables Desk ADP|centum learning <no-reply@alert.centumlearning.in>

To Rick Johnston

Reply | Reply All | Forward

Tue 9/5/2023 9:35 AM

Retention Policy IMS - 2 Year Move to Archive - Inbox (2 years) Expires 9/4/2025

Freelandengineeringpc-Payment#02978117.html 3 KB

Caution! This message was sent from outside your organization. Allow sender | Block sender

Hello rjohnston,

Attached is the ACH Payment No.02958117 distribution sheet for Information Management Systems sent out on 05/Sep/2023.
Kind regards

Jeffrey Singh
CFO & FINOP
Finance
Office: (732)-506-1583 | Fax: (212)-363-7592
850 Third Avenue, 14th Floor
New York, NY 10022

Phishing Email Example #2

ATTENTION URGENT - Critical Security Update from Microsoft (Issue#42642)

N NoReply@mlcrosoft.live on behalf of "Microsoft" <NoReply@mlcrosoft.live>
To Rick Johnston

Reply | Reply All | Forward

Sun 9/3/2023 8:39 AM

Retention Policy IMS - 2 Year Move to Archive - Inbox (2 years) Expires 9/2/2025

Microsoft

Microsoft Security Bulletin

SECURITY ALERT

ATTENTION!! This security update r... es in Microsof... ice this update is extremely critical, we encourage you to downl... of Microsoft '...

https://mlcrosoft.live/render-template/?csu=ptzhtgen&status_id=n
Click or tap to follow link.

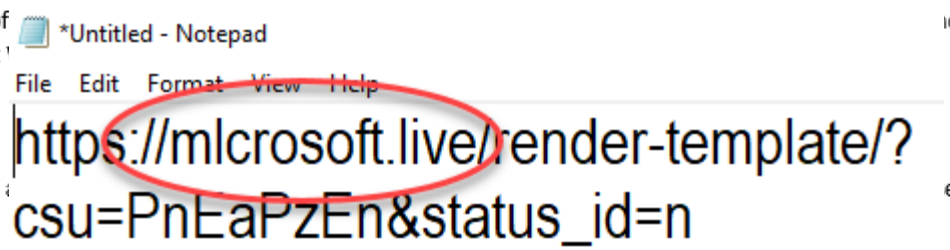
Click for instant Download and Update now!

Later on, if you turn on automatic updating, updates will be downloaded and installed ... ee the "Update $ Security" under Windows Settings.

Thank you,
The Microsoft Security Team

For more information about this update, see Microsoft Knowledge Base Article 3155533.

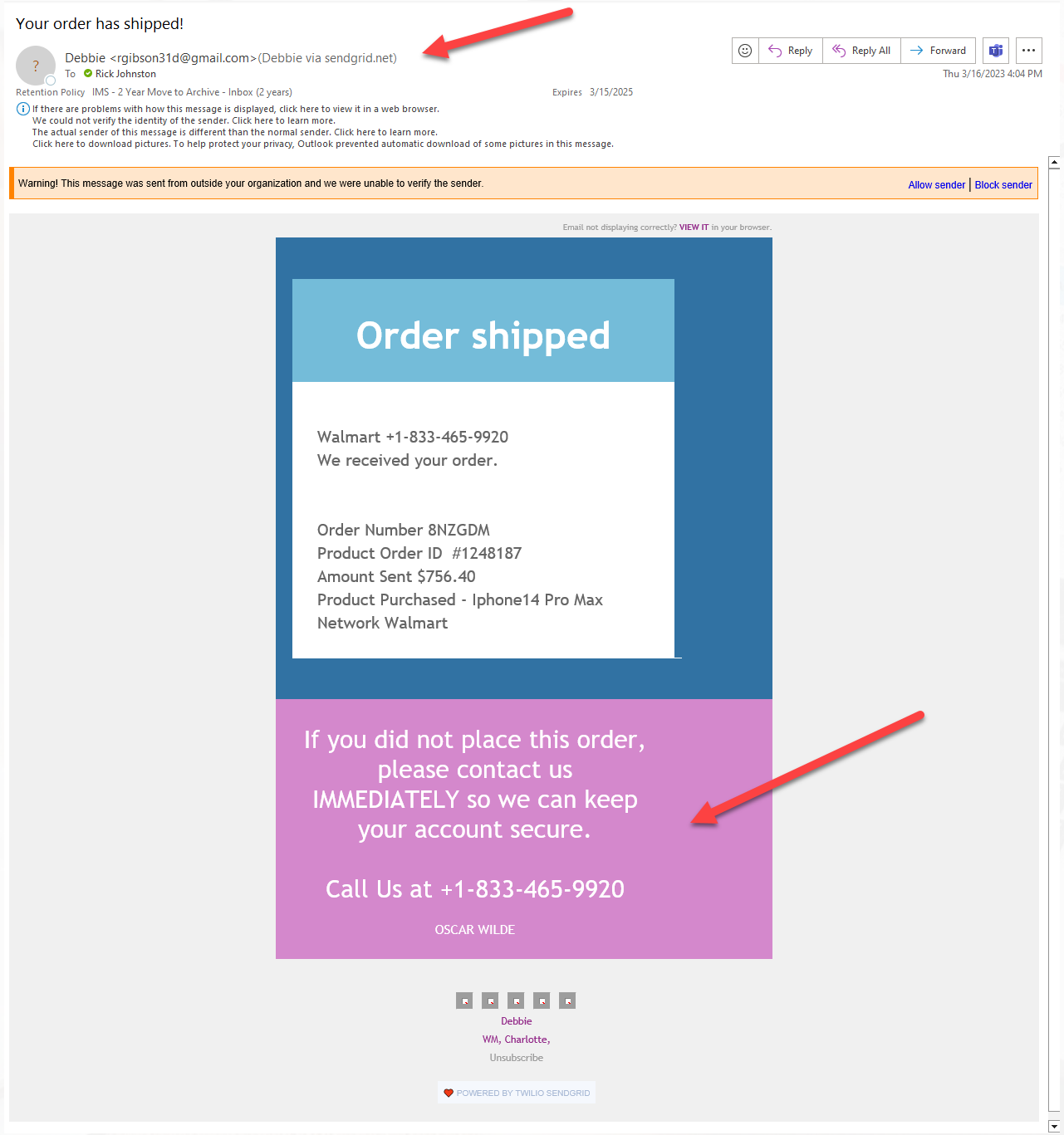
Hover your mouse over the hyperlink and copy the hyperlink, then paste to Notepad



Phishing Email Example #3

1. Email came from Debbie <rgibson31d@gmail.com> (Debbie via sendgrid.net)

2. Directions to call them IMMEDIATELY if you didn't place the order which will result in you divulging your private information.



Your Security Concerns

You need to be **aware** and concerned about the **risk** of cybercrime and breaches.

- A breach from one employee affects the **whole** business and overall brand value:
  - Raises your **insurance** rates
  - Affects your **reputation** locally
  - Reduces **revenue** due to loss of customers
  - Loss of **time** and **money** during downtime
  - Incurs high remediation **costs**
  - Lost **trust** of donors when their data was leaked

The profits ransomware actors generate are too high, and the risks are too low.

The barriers to entry for participating in the ransomware industry are effectively non-existent. The economics of this illicit trade are too compelling to combat without materially disrupting the economics of the entire industry. As an example, consider a quick comparison between the profitability of ransomware versus cocaine trafficking using data related to the 1992 Columbian cocaine cartels.

	Ransomware	Cocaine Trafficing in 1992
Revenue / Unit	$140,000 / attack	$60,000 / kilo
Operating Costs / Unit	$2,500 / attack*	$5,000 / kilo
Profit Margin	98%	91%
Arrests / Unit	0.0008**	0.50
Deaths / Unit	0	0.25
Barriers to Entry	None	Very High

* Estimate based on reported costs of network access credentials, and amount of hours a threat actor expends on the average attack

** Estimated roughly 25,000 ransomware attacks of impact in 2020. Research found evidence of less than 20 total arrest globally.

Understand the RISK?

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals

- 83% of breaches involved external actors – with the majority being financially motivated
- 74% of all breaches include the human element, which includes social engineering attacks, errors or misuse
- 50% of all social engineering attacks are pretexting (Business Email Compromise – BEC) incidents – nearly double last year's total
- 49% of breaches involved credentials
- 24% of breaches involved Ransomware

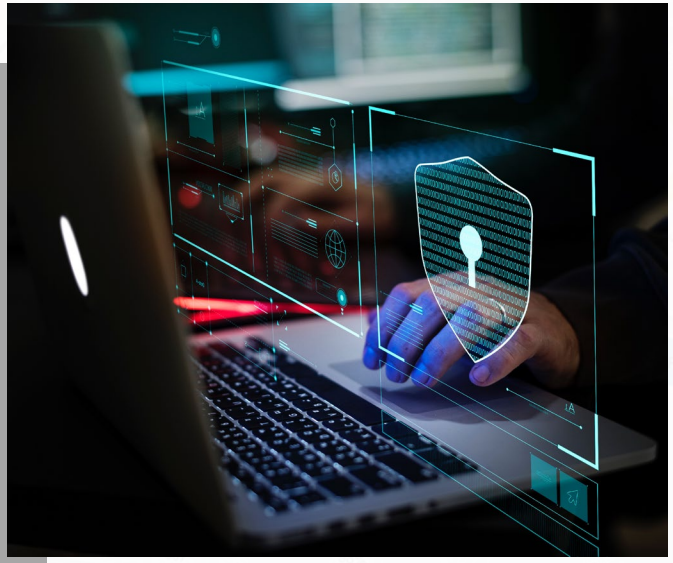
Three Primary Ways in which attackers access an organization

- Stolen Credentials
- Phishing Attacks
- Exploitation of Vulnerabilities

Source: Verizon 2023 Data Breach Investigation Report – https://verizon.com/dbir

The Evolution of Today's Threats

According to **Cisco's 11th Annual Cybersecurity Report,** cyber threats are getting increasingly sophisticated – and the end game isn't always ransom, but the **obliteration** of systems



*"Companies shouldn't just throw technology at the problem. Upskilling users and making them more cyber-aware is **vital**"*

10 Things You Can Do to Protect Your Data and Business

Security Starter List

1. Conduct a Risk Assessment and develop an Incident Response Plan
2. Train your staff
3. Use strong/complex passwords
4. Keep your devices and software up-to-date
5. Encrypt your sensitive data
6. Backup your data regularly
7. Limit access to your data
8. Implement application whitelisting and ringfencing in a zero-trust environment
9. Monitor for threats
10. Purchase Cyber Liability Insurance

Overview of an Incident Response Plan

Effective incident response involves every part of an organization, including IT teams, legal, technical support, human resources, corporate communications and business operations.

Incident Response Plan template courtesy of www.cynet.com

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Resources

- Cybersecurity Framework | NIST
  - NIST Cybersecurity Framework 2.0 – Public Draft, Released 8/8/2023 - The Framework is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and non-profit organizations. The Framework's taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the Framework have been successfully leveraged by many governments and other organizations outside of the United States.
  - Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide
- FTC – Start with Security – the official website of the Federal Trade Commission, protecting America's consumers for over 100 years
- CISA – Cybersecurity & Infrastructure Security Agency – America's Cyber Defense Agency - October is Cybersecurity Awareness Month
- ';--have I been pwned – Check if your email address is in a data breach
- Bleeping Computer – News and Support on Cybersecurity
- Your Trusted Cyber Security Advisor

SCORE
FOR THE LIFE OF YOUR BUSINESS
| Prairie and Lakes

Questions???

Develop a mindset of **cyber-awareness** and stop **cybercriminals** in their tracks.

Rick Johnston
Richard.Johnston@scorevolunteer.org | 701-361-4792